ASA Häufig gestellte Fragen: Warum sendet die ASA Pakete ohne IPS-Richtlinienkonfiguration an das IPS-Modul?

Inhalt

Einführung

In diesem Dokument wird erläutert, warum die Cisco Adaptive Security Appliance (ASA) Datenverkehr zur Überprüfung an ein integriertes Servicemodul senden könnte, wenn die Konfiguration keine IPS-Modulrichtlinie (Intrusion Prevention System) enthält.

F. Warum sendet die ASA Pakete zur Überprüfung an das IPS-Modul, wenn keine IPS-Richtlinie konfiguriert ist?

Antwort:

Es ist möglich, dass eine Verbindung aufgebaut wurde, um Datenverkehr zum IPS-Modul zur Überprüfung zu senden, wenn die ASA konfiguriert wurde, und diese Verbindung noch aktiv ist.

Beispielsweise verfügt ein Kunde mit einem ASA5515-IPS über keine konfigurierte Richtlinie in einer Richtlinienzuordnung zum Senden des Datenverkehrs an das Software-IPS-Modul. Der Datenverkehr kommt jedoch vom ASA-Modul an.

Wenn Sie die Paketanzeigefunktion des IPS verwenden, können Sie den Datenverkehr sehen, der von der ASA zum IPS gelangt:

```
14:34:38.341927 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.341992 IP 192.168.1.2.1719 > 192.168.10.39.1888: UDP, length 128
14:34:38.345031 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
14:34:38.345068 IP 192.168.1.2.1719 > 192.168.110.39.1888: UDP, length 34
```

Die Schnittstellenstatistiken an der IPS-Sensorschnittstelle wurden gelöscht, und es wurden Pakete empfangen:

```
sensor#  show interfaces portChannel
```

```
MAC statistics from interface PortChannel0/0
Interface function = Sensing interface
Description =
Media Type = backplane
Default Vlan = 0
InlineMode = Unpaired
Pair Status = N/A
Hardware Bypass Capable = No
Hardware Bypass Paired = N/A
Link Status = Up
Admin Enabled Status = Enabled
Link Speed = N/A
Link Duplex = N/A
Missed Packet Percentage = 0
Total Packets Received = 128
Total Bytes Received = 17904
Total Packets Transmitted = 128
Total Bytes Transmitted = 17904
```

Das Problem besteht darin, dass der ASA irgendwann einmal eine Konfiguration hinzugefügt wurde, um Datenverkehr an das IPS-Modul zu senden, und dass die Verbindungen nicht entfernt wurden, nachdem die IPS-Konfiguration auf der ASA entfernt wurde. Dies ist bei Nicht-TCP-Protokollen üblich, die fortlaufend Datenverkehr weiterleiten.

Geben Sie auf der ASA den Befehl **show conn** ein, um festzustellen, ob die Pakete, die Sie auf dem IPS-Modul sehen, Verbindungseinträge enthalten. Um die Betriebszeiten anzuzeigen, geben Sie den Befehl **show conn detail ein**. Um sicherzustellen, dass die Verbindungen nicht zum IPS umgeleitet werden, müssen Sie möglicherweise den **Befehl clear conn *<address>*** auf der ASA eingeben, um diese spezifischen Verbindungen zu löschen:

```
ASA# clear conn address 192.168.1.2
3 connection(s) deleted.
ASA#
```

Zugehörige Informationen

- Technischer Support und Dokumentation - Cisco Systems